REMARKS

In the Office Action mailed June 9, 2009, the Examiner noted that claims 1-19 were pending and rejected claims 1-19. Claim 1 has been amended, no claims have been canceled, and, thus, in view of the foregoing, claims 1-19 remain pending for reconsideration which is requested. No new matter has been added. The Office's rejections and objections are addressed below.

CLAIM OBJECTION

Claim 1 stands objected to for informalities. In particular, the Office asserts that that it is unclear if the "multicast packet" positively contains said enciphered data and current use identifier. The Applicant has amended the claim to overcome the rejection.

Withdrawal of the rejection is respectfully requested.

REJECTIONS under 35 U.S.C. § 112

Claims 1-19 stand rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement. In particular, the Office asserts that "said current use cipher key being ***separate*** from said current use decipher key," as in claim 1 is not disclosed.

However, ¶ 0177 of the printed publication version of

the Specification states

> The content server 11 holds as a key data, a set of keys (**a cipher key and a decipher key**), a key identifier for the keys, and a remaining effective time of the keys about each of current use keys and next use keys, and transmits the key data to the key management server 31 as a key data message 71.

Thus, the Specification sets out that the contents server holds a cipher key and decipher key (i.e. separate keys), not a single key for both enciphering and deciphering.

Therefore, the claim as written is supported by the Specification.

Withdrawal of the rejection is respectfully requested.

REJECTIONS under 35 U.S.C. § 101

Claims 1-19 stands rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. In particular, the Office asserts that the claims are to software per se.

Claim 1 recites "a delivery server which enciphers delivery data … a key management server which is connected with said delivery server through a network … ***a client terminal*** which is connected with said delivery server and said key management server through said network…." (Emphasis added) The Applicants acknowledge that the term "server" as in the first two features in common usage may refer to either hardware or software. However, "a client terminal" is hardware and thus renders the

claim statutory. The Free Online Dictionary of Computing (foldoc.org) states that a terminal is:

> 1. <*hardware*> An electronic or electromechanical device for entering data into a computer or a communications system and displaying data received. Early terminals were called teletypes, later ones VDUs. Typically a terminal communicates with the computer via a serial line.
>
> 2. <*electronics*> The end of a line where signals are either transmitted or received, or a point along the length of a line where the signals are made available to apparatus.
>
> 3. <*electronics*> Apparatus to send and/or receive signals on a line.

Thus, the claim as written is statutory.

Withdrawal of the rejections is respectfully requested.

REJECTIONS under 35 U.S.C. § 102

Claims 1-4, 18 and 19 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Caronni, U.S. Patent No. 6,049,878. The Applicants respectfully disagree and traverse the rejection with an argument.

Caronni discusses secure multicast system including a traffic distribution component coupled to the sending entity and each of the receiving entities, where the traffic distribution component supports a connectionless datagram protocol and a participant key management component operates within each receiver entity where the participant key management component holds a first key that is shared with the sender and all of the

receiving entities, and a second key that is shared with the sender and at least one but less than all of the receiving entities.

On page 4 of the Office Action, it is asserted that Caronni, col. 5, lines 1-12 and Fig. 2 disclose "a delivery server which enciphers delivery data by using a current use cipher key to generate enciphered data **and transmits a multicast packet containing said enciphered data and a current use key identifier**, said current use key identifier identifies a pair of said current use cipher key and a current use decipher key as current use keys, said current use cipher key being separate from said current use decipher key," as in claim 1.

However, Caronni, col. 5, lines 1-12 states

> a symmetric traffic encryption key (TEK) that is generated by the group key management component 108. The traffic encryption component 106 uses the TEK to encrypt data that is to be sent out. In the example of FIG. 1, the traffic encryption component receives IP packets from the transport layer 104 (which in turn include data messages generated by sending multicast application 102), ***encrypts the entire IP packet, and adds new header information (unencrypted) to direct the packet. This encryption can be performed using any available encryption algorithm or combination of algorithms*** including DES, RC4, other block stream ciphers, and the like.

Thus, Caronni does discuss a header which is used to direct the packet, but is does not state that the header contains **a current use key identifier**, where the identifier identifies a pair of said current use cipher key and a current use decipher key as

current use keys. Caronni is completely silent as to such a feature. Neither is such a feature implicit as the reference states encryption can be performed using any available encryption algorithm without stating how such an algorithm is implemented.

Further, with reference to Fig. 2, col. 8, lines 1-20 state

> Normal data transfer in accordance with the present invention is sent in packets 200 having a format shown in FIG. 2. **Each packet includes an association ID field which gives the ID of the group key manager 108 or sender 100 originating the data packet 200.** Each packet 200 also includes **a key version field and a key revision field. The key encryption key revision number may be a single bit which is set (i.e., placed in a one level) by join operations and reset after a leave operation has caused this key to be replaced.** Additional headers which may comprise one or more header fields used in the traffic distribution component are also provided. The encrypted payload typically comprises an encrypted IP packet (e.g., a SKIP packet). As each packet is received by a receiving participant 101, **the participants 101 can detect key revision changes and use the one-way function to generate a revised key.** Each packet may also indicate version changes which involve new keys, but the new key is provided in a separate update message described hereinbelow. The participant 101 can also request version updates if it appears they have missed messages due to damaged or dropped packets which are typical in an Internet application.

Thus, the associate ID field is not a current use identifier as it does not identify a cipher key and decipher key. The same is true of the key version and key revision, they likewise don't identify a cipher/decipher pair of values.

On page 4 of the Office Action, it is asserted that

Caronni, col. 6, lines 1-39 disclose "a key management server which is connected with said delivery server through a network, holds as a current use key data, a set of said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as a current use decipherment key data in response to a current use key data request," as in claim 1.

However, as discussed above, there is no current use key identifier use din the Caronni reference.

On pages 4 and 5 of the Office Action, it is asserted that Caronni, col. 4, lines 1-11 and 32-42; col. 6, lines 51-56; and col. 10, lines 1-12 disclose " a client terminal which is connected with said delivery server and said key management server through said network, receives said multicast packet from said delivery server, issues said current use key data request to said key management server to receive said current use decipherment key data from said key management server, holds said set of said current use decipher key and said current use key identifier, and deciphers said enciphered data contained in said multicast packet by using said current use decipher key when said current use key identifier contained in said multicast packet is coincident with said current use key identifier held in said client terminal," as in claim 1.

However, as quotes above with respect to Caronni, col.

8, lines 1-20 "the participants 101 can detect key revision changes and use the one-way function to generate a revised key." Thus, in Caronni, the client terminal does not "issues said current use key data request to said key management server to receive said current use decipherment key data from said key management server." In Caronni, the user simply uses a one-way function to generate a key.

For at least the reasons discussed above, claim 1 and the claims dependent therefrom are not anticipated by Caronni.

Withdrawal of the rejections is respectfully requested.

REJECTIONS under 35 U.S.C. § 103

Claims 5-17 stand rejected under 35 U.S.C. § 103(a) as being obvious over Caronni in view of Larsen, U.S. Patent No. 7,068,791. The Applicants respectfully disagree and traverse the rejection with an argument.

Larsen adds nothing to the deficiencies of Caronni as applied to the independent claims. Therefore, Caronni and Larsen, taken separately or in combination, fail to render obvious the elements of claims 5-17.

Withdrawal of the rejections is respectfully requested.

SUMMARY

It is submitted that the claims satisfy the requirements of 35 U.S.C. §§ 112, 101, 102 and 103. It is also submitted that claims 1-19 continue to be allowable. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/James J. Livingston, Jr./
Reg. No. 55,394
209 Madison Street, Suite 500
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JJL/jad